

## Defense Acquisition Regulations System, DoD

## 252.204-7008

(iii) 252.222-7007, Representation Regarding Combating Trafficking in Persons, as prescribed in 222.1771. Applies to solicitations with a value expected to exceed the simplified acquisition threshold.

(iv) 252.225-7042, Authorization to Perform. Applies to all solicitations when performance will be wholly or in part in a foreign country.

(v) 252.225-7049, Prohibition on Acquisition of Commercial Satellite Services from Certain Foreign Entities—Representations. Applies to solicitations for the acquisition of commercial satellite services.

(vi) 252.225-7050, Disclosure of Ownership or Control by the Government of a Country that is a State Sponsor of Terrorism. Applies to all solicitations expected to result in contracts of \$150,000 or more.

(vii) 252.229-7012, Tax Exemptions (Italy)—Representation. Applies to solicitations when contract performance will be in Italy.

(viii) 252.229-7013, Tax Exemptions (Spain)—Representation. Applies to solicitations when contract performance will be in Spain.

(ix) 252.247-7022, Representation of Extent of Transportation by Sea. Applies to all solicitations except those for direct purchase of ocean transportation services or those with an anticipated value at or below the simplified acquisition threshold.

(2) The following representations or certifications in SAM are applicable to this solicitation as indicated by the Contracting Officer: [Contracting Officer check as appropriate.]

(i) 252.209-7002, Disclosure of Ownership or Control by a Foreign Government.

(ii) 252.225-7000, Buy American—Balance of Payments Program Certificate.

(iii) 252.225-7020, Trade Agreements Certificate.

Use with Alternate I.

(iv) 252.225-7031, Secondary Arab Boycott of Israel.

(v) 252.225-7035, Buy American—Free Trade Agreements—Balance of Payments Program Certificate.

Use with Alternate I.

Use with Alternate II.

Use with Alternate III.

Use with Alternate IV.

Use with Alternate V.

(e) The offeror has completed the annual representations and certifications electronically via the SAM Web site at <https://www.acquisition.gov/>. After reviewing the ORCA database information, the offeror verifies by submission of the offer that the representations and certifications currently posted electronically that apply to this solicitation as indicated in FAR 52.204-8(c) and paragraph (d) of this provision have been entered or updated within the last 12 months, are current, accurate, complete, and applicable to this solicitation (including the business size standard applicable to the NAICS code referenced for this solicitation), as of the date of this offer, and are incorporated in this offer by reference (see FAR 4.1201); except for the changes identified below [offeror to insert changes, identifying change by provision number, title, date]. Any changes provided by the offeror are applicable to this solicitation only, and do not result in an update to the representations and certifications located in the SAM database.

FAR/DFARS provision No.	Title	Date	Change

Any changes provided by the offeror are applicable to this solicitation only, and do not result in an update to the representations and certifications posted on ORCA.

(End of provision)

[76 FR 58141, Sept. 20, 2011, as amended at 76 FR 71464, Nov. 18, 2011; 77 FR 19130, Mar. 30, 2012; 77 FR 30357, May 22, 2012; 77 FR 35881, June 15, 2012; 77 FR 43470, July 24, 2012; 78 FR 28758, May 16, 2013; 78 FR 30232, May 22, 2013; 79 FR 17446, Mar. 28, 2014; 79 FR 45664, Aug. 5, 2014; 79 FR 73490, Dec. 11, 2014; 80 FR 5001, Jan. 29, 2015]

### 252.204-7008 Compliance with safeguarding covered defense information controls.

As prescribed in 204.7304(a), use the following provision:

#### COMPLIANCE WITH SAFEGUARDING COVERED DEFENSE INFORMATION CONTROLS (AUG 2015)

(a) *Definitions.* As used in this provision—

*Controlled technical information, covered contractor information system, and covered defense information* are defined in clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting.

(b) The security requirements required by contract clause 252.204-7012, Covered Defense Information and Cyber Incident Reporting, shall be implemented for all covered defense

information on all covered contractor information systems that support the performance of this contract.

(c) If the Offeror proposes to deviate from any of the security requirements in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations," <http://dx.doi.org/10.6028/NIST.SP.800-171> that is in effect at the time the solicitation is issued or as authorized by the Contracting Officer, the Offeror shall submit to the Contracting Officer, for consideration by the DoD CIO, a written explanation of—

(1) Why a particular security requirement is not applicable; or

(2) How an alternative but equally effective, security measure is used to compensate for the inability to satisfy a particular requirement and achieve equivalent protection.

(d) An authorized representative of the DoD CIO will approve or disapprove offeror requests to deviate from NIST SP 800-171 requirements in writing prior to contract award. Any approved deviation from NIST SP 800-171 shall be incorporated into the resulting contract.

(End of provision)

[80 FR 51744, Aug. 26, 2015]

**252.204-7009 Limitations on the use or disclosure of third-party contractor reported cyber incident information.**

As prescribed in 204.7304(b), use the following clause:

**LIMITATIONS ON THE USE OR DISCLOSURE OF THIRD-PARTY CONTRACTOR REPORTED CYBER INCIDENT INFORMATION (AUG 2015)**

(a) *Definitions.* As used in this clause—

*Controlled technical information* means technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. Controlled technical information would meet the criteria, if disseminated, for distribution statements B through F using the criteria set forth in DoD Instruction 5230.24, Distribution Statements on Technical Documents. The term does not include information that is lawfully publicly available without restrictions.

*Covered defense information* means unclassified information that—

(1) Is—

(i) Provided to the contractor by or on behalf of DoD in connection with the performance of the contract; or

(ii) Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract; and

(2) Falls in any of the following categories:

(i) *Controlled technical information.*

(ii) *Critical information (operations security).* Specific facts identified through the Operations Security process about friendly intentions, capabilities, and activities vitally needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequences for friendly mission accomplishment (part of Operations Security process).

(iii) *Export control.* Unclassified information concerning certain items, commodities, technology, software, or other information whose export could reasonably be expected to adversely affect the United States national security and nonproliferation objectives. To include dual use items; items identified in export administration regulations, international traffic in arms regulations and munitions list; license applications; and sensitive nuclear technology information.

(iv) Any other information, marked or otherwise identified in the contract, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Governmentwide policies (e.g., privacy, proprietary business information).

*Cyber incident* means actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein.

(b) *Restrictions.* The Contractor agrees that the following conditions apply to any information it receives or creates in the performance of this contract that is information obtained from a third-party's reporting of a cyber incident pursuant to DFARS clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting (or derived from such information obtained under that clause):

(1) The Contractor shall access and use the information only for the purpose of furnishing advice or technical assistance directly to the Government in support of the Government's activities related to clause 252.204-7012, and shall not be used for any other purpose.

(2) The Contractor shall protect the information against unauthorized release or disclosure.

(3) The Contractor shall ensure that its employees are subject to use and non-disclosure obligations consistent with this clause prior to the employees being provided access to or use of the information.

(4) The third-party contractor that reported the cyber incident is a third-party beneficiary of the non-disclosure agreement